Safe Internet, Happy Future!

Information Security
in Korea

CONTENTS

IoT
IPTV
Cloud
Big
Data
LTE
NFC
Mobile
SMS

CHAPTER 1 National Information Security System of Korea

In responding to cyber threats, the National Security Office (NSO) of the Blue House plays the role of a cyber security control tower, while the National Intelligence Service (NIS) oversees operations at the working level in conjunction with the competent authorities designated in the private, public, and military sectors respectively.

To fortify the cyber security control tower functions of the NSO of the Blue House, a presidential office of cyber security has been established, along with a cyber security governance framework in which the development, implementation and evaluation of national cyber security policies have been unified.

The NIS oversees cyber security operations at the working level, whereas the National Cyber Security Center (NCSC) under the control of the NIS prevents cyber threats and investigates internet security incidents in the government and public sectors; gathers, analyzes and disseminates intelligence on cyber threats; holds Strategy Meetings; and develops cyber security master plans, etc. In addition, the NCSC operates a joint response team composed of representatives from the private, public and military sectors as a part of the national cyber security response system.

The Ministry of National Defense (MND) addresses cyber security issues relevant to the national defense through its Cyber Warfare Command and Defense Security Command by working to prevent cyber threats, responding to cyber security incidents in the field, waging cyber warfare when necessary, and developing the applicable technologies.

The Ministry of Science, ICT and Future Planning (MSIP) is responsible for cyber security activities in the private sector. The MSIP recently developed a comprehensive national cyber security policy package (July 4, 2013) involving the relevant government

[1] As the number of cyber attacks increased dramatically, exemplified by the disruption of the Internet service on January 25, 2003, the Government established the NCSC in the NIS.

ministries in a bid to systematically respond to cyber threats to national security, and established the IoT Information Security Roadmap (October 31, 2014) to promote a secure IoT environment.

The Korea Internet & Security Agency (KISA) is responsible for preventing cyber threats, responding to cyber security incidents in the private sector, raising public awareness of cyber security issues, nurturing information security industries/resources, and promoting the development of information security technologies.

KOREA
IoT
IPTV
SMS
Cloud
Big
Data
LTE
NFC
Mobile

CHAPTER 2 Information Security Legal/ Institutional Framework

Section 1 Laws/Regulations relating to Information Security in the Public Sector

The information security implementation framework of the public sector is governed by 「The National Cyber Security Management Regulations」.

Cyber security policies and the management thereof are overseen and coordinated by the director of the NIS in consultation with the head of the applicable central administrative agency. Furthermore, the National Cyber Security Strategy Meeting, National Cyber Security Countermeasure Meeting, and NCSC have all been placed under the control of the director of the NIS.

The head of the central administrative agency develops, implements, guides, and supervises cyber security countermeasures in their respective jurisdictions. The heads of the central administrative agency, local municipalities and public authorities establish and operate security control centers respectively and notify the head of the NSO and the director of the NIS of intelligence concerning potential cyber security threats immediately upon its gathering.

Generally, a head of a central administrative agency who becomes aware of a cyber security intrusion or signs thereof takes the necessary measures to minimize the damage and informs the head of the NSO and the NIS director of the cyber security incident. The NIS director may conduct an investigation to identify the cause of such an incident and organize a dedicated cyber crisis response team if the damage is serious enough. The NIS director also notifies the NSO of the damage caused by a cyber attack and the ongoing responses, whereas the head of NSO confirms the applicable details and reports them to the President. As for R&D, the NIS director enforces any initiatives required for cyber security R&D efforts, and the head of the central administrative agency may commission the National Security Technology Research Institute (NSR) to conduct the applicable R&D projects.

Section 2 Laws/Regulations relating to Information Security in the Private Sector

The information security governance structure of the private sector is governed by 「The Act on the Promotion of Information and Communications Network Utilization and Information Protection, etc.」.

Information and communications service providers covered by the criteria set forth by Presidential decree in terms of the number of employees and/or users are required to appoint chief information security officers and report to the MSIP. Such information and communications service providers must put protective arrangements in place to secure the stability and reliability of the information and communications infrastructure used to deliver information and communications services. One of the principal responsibilities of the MSIP is to issue information security guidelines. The Minister may recommend protective measures that are deemed to be required as per the preliminary information security inspection standards, assign an information security management classification, and certify the operators of information security management systems.

Information and communications service providers and the Internet Data Center (IDC) must report information security incidents immediately to the MSIP or KISA. The Minister may organize a joint investigation team composed of representatives from government and private sector organizations to analyze the cause of a critical security incident affecting the information and communications infrastructure of the applicable service provider. The Minister conducts emergency measures to gather and disseminate intelligence on information security intrusions, prevents and/or warns of potential security incidents, and has the KISA perform such roles where appropriate.

Section 3 Laws/Regulations relating to Information Security for Critical Information and C/mmunications Infrastructures

The information security framework for critical information and communications infrastructures is operated by the Committee for the Protection of Information and Communications Infrastructure established under 「The Act on the Protection of Information & Communications Infrastructure」.

The Committee for the Protection of Information and Communications Infrastructure is chaired by the Head of the Office for Government Policy Coordination, staffed by vice ministers, and mandated to deliberate on matters pertaining to the protection of critical information and communications infrastructures.

The MSIP and the NIS director may notify measures and plans for protecting critical information and communications infrastructures to the head of the central administrative agency and verify the implementation status of such protective measures. The MSIP, NIS director, NSR, KISA, Information Sharing and Analysis Center (ISAC), and information security consulting firms develop protection measures for critical information and communications infrastructures, prevent and assist recovery from information security incidents, and provide technical support for the implementation of protection measures and recommendations.

The central administrative agency designates information and communications facilities deemed to require protection from electronic intrusions as critical information and communications infrastructures. The MSIP and the NIS director may recommend the central administrative agency to designate critical information and communications infrastructures where necessary. The central administrative agency may develop/implement protection plans for critical information and communications infrastructures under their jurisdiction, protection guidelines for such infrastructures, and order or recommend protection measures to be taken by the applicable management organizations.

Organizations that wish to provide intelligence on security vulnerabilities and drawbacks, and operate real-time alarm and analytics systems to protect information and communications infrastructures in the fields of banking, communications, etc. may establish and operate information sharing and analysis centers.

Section 4 Information Security Industry Promotion Act

「The Information Security Industry Promotion Act」 was adopted in June 2015 to establish the foundation for the information security industry in Korea and to foster its competitiveness.

The Act contains provisions for the expansion of the information security market in Korea, and promotes demand and creates new markets for information security products and services development, provides systematic education and management of information security specialist resources, and fosters information security companies, etc.

① The Act stipulates that the MSIP shall develop and implement promotion plans to set policy objectives and directions regarding the promotion of the information security industry. Furthermore, government organizations shall submit demands for information security products and services and system implementation plans to the Minister in advance in order to boost the overall demand for information security in the public sector.

② Public authorities, etc. shall try to pay the appropriate procurement prices to guarantee the quality of information security systems, and the MSIP shall ensure that unfair procurement practices are prevented.

③ Required support may be extended to organizations mandated to review and certify information security readiness for the security of information and communications service users.

④ The MSIP may implement programs to promote and standardize the development of and investment in information security industrial technologies, and establish and implement initiatives for the nurturing of information security specialist resources.

⑤ Information security product and technology performance evaluations may be supported to ensure their quality, promote the distribution thereof, protect users, and foster convergence industries. Excellent information security products and services may be designated annually and procured preferentially. Excellent information service companies may also be designated annually and entitled to policy loans, export tax relief, and so forth.

⑥ The MSIP may establish an agency dedicated to the promotion of the information security industry or delegate such a function to a third party organization, and authorize the founding of an information security industry association.

⑦ The Government shall reflect information security performance (i.e. managerial, technical, and physical information security measures and the performance thereof) through an evaluation of the management performance of public sector organizations.

Section 5 The Status of Laws/Regulations by Purpose of Enactment and Function

The laws and regulations governing information security in Korea are divided according to the purpose of their enactment and the functions thereof into 1) those governing national confidential information, 2) those governing the prevention of the divulgence of critical information to foreign countries, 3) those governing digital signature and authentication, 4) those governing the security of information and communications networks and systems, 5) those governing the punishment of information security intrusions, and 6) those governing the protection of personal information as shown in the following table.

Major Laws/Regulations Governing Information Security

Category	Names of Laws/Regulations
Protection of national confidential information	Including but not limited to : • Military Secret Protection Act • Military Criminal Act
Prevention of divulgence of critical information to foreign countries	Including but not limited to : • Act on Prevention of Divulgence and Protection of Industrial Technology • Technology Transfer and Commercialization Promotion Act • Promotion of Technology Projects for Joint Civilian and Military Use Act • Unfair Competition Prevention and Trade Secret Protection Act
Digital signature and authentication	Including but not limited to : • Digital Signature Act • Electronic Government Act
Protection of information and communications networks and systems	Including but not limited to : • Framework Act on National Informatization • Act on the Protection of Information and Communications Infrastructure • Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. • Electronic Government Act • Framework Act on Electronic Documents and Transactions • National Cyber Security Management Regulations
Punishment of information security intrusions	Including but not limited to : • Act on the Protection of Information and Communications Infrastructure • Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. • Electronic Trade Facilitation Act • Criminal acts
Protection of personal information	Including but not limited to : • Personal Information Protection Act • Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. • Use and Protection of Credit Information Act
Information Security Industry	Including but not limited to : • Information Security Industry Promotion Act • Framework Act on National Informatization

IoT
Big
Data
LTE
IPTV
SMS
Mobile
Cloud
NFC

CHAPTER 3

Information Security policies

Section 1 IoT Information Security Roadmap

It is anticipated that the threats already existing in cyber space will spread to the Internet of Things (IoT) environment in which all things and data (including personal information) are connected with each other. In particular, as the application of IoT involving home appliances, medical systems and automobiles, etc. interacts directly with all things in our daily lives, IoT security threats may be deadly enough to threaten human life by causing system malfunctions or failures, etc. as well as being either impossible or extremely costly to address ex post, which attests to the criticality of implementing countermeasures to thwart them.

Accordingly, under the principle that security must be guaranteed if the IoT is to make everyone's life safe and convenient as a future growth engine and contributor to the creative economy, the Government gathered feedback extensively from all corners of the academic, industrial and research communities and the relevant government organizations with the aim of developing an IoT Information Security Roadmap for fostering a secure IoT user environment.

The roadmap envisions ① the creation of a security-embedded infrastructure, ② the development of nine market-leading security technologies for the global convergence security market, and ③ enhancement of the IoT security industry's competitiveness, to be realized in phases by 2018 in a bid to turn Korea into the world's best smart and secure nation.

The IoT information security roadmap prescribes first of all that security will be embedded in seven IoT application categories including home/electronic appliances, medical science (including foods/beverages), transportation (automobile, aviation, railroads, etc.), environment/disaster recovery, manufacturing, construction and energy from the IoT product/service design phase to distribution, supply and the maintenance thereof. Second, the Secure Dome project will be implemented to develop nine core security technologies aligned with IoT characteristics (lightweight, low power consumption, and super connectivity) in each of four layers (device/network/service/platform) to ensure secure protection of IoT products and services. Last but not least, IoT convergence security POC (proof of concept) projects will be implemented to bolster the competitiveness of the IoT security industry, promote demand for IoT security products and services, and nurture IoT security brains as ICT-security convergence resources through multi-disciplinary interfaces.

Section 2 K-ICT Security Development Strategy

As the era of super-connectivity and ICT convergence in which everything is connected with everything else via the Internet, and as conventional industries and ICT are converged at an accelerated pace, cyber threats are evolving beyond the mere leakage of personal information or simple financial scams to the extent of fanning national or social confusion and posing threats to national security. However, voluntary efforts to spur public awareness of the importance of information security are still inadequate in Korea, while the fundamental foundation - including the industrial base, specialist resources and R&D investment - is still immature with regard to information security as most information security companies in Korea are small or medium-sized enterprises.

Accordingly, the MSIP established the K-ICT security development strategy in a drive to position information security as the basis for public life and overall industrial domains by drastically overhauling the information security paradigm and fostering the information security industry as a new growth engine of the creative economy. The Ministry plans to invest KRW 810 billion in total by 2019 to implement the following four overarching tasks:

➀ Create future growth drivers by strengthening the foundations of the information security industry;

➁ Develop original security technologies to capitalize on the first-mover advantage in the global market;

➂ Nurture elite security resources and promote a culture of rigorous information security practices; and

➃ Increase investment to improve the resilience of cyber security.

Each of the tasks outlined above are presented as follows in greater detail:

① First, to create future growth drivers by strengthening the foundations of the information security industry, it is necessary to ensure the objectivity of quality via information security performance evaluation, develop product benchmarking standards, and provide performance test results to clients in the public sector during procurement processes in order to encourage them to select excellent products. In addition, to ensure an appropriate compensation calculation scheme for security service continuation and maintain the security of information security products, an information security service compensation estimation guideline will be developed. In so doing, the Ministry plans to eliminate the vicious cycle in which a lack of appropriate compensation for information security service weighs heavily on the profitability of information security enterprises, as well as compromising the competitiveness of technologies and products as a result of the “brain drain” phenomenon.

Second, to encourage business organizations to invest in security and implement proactive information security measures, the Ministry plans to provide incentives for investment in information security in such forms as tax relief and preferential treatment in connection with the public sector procurement processes and R&D initiatives, and will consider and publish enterprise information security status information in order to disclose the information security status (i.e to promote transparency in terms of resources, organizations, and education, etc.). In particular, the Ministry plans to accord greater priority to information security investment in evaluation programs in a bid to bolster the security level of leading private enterprises (ISMS-certified companies, mobile telecom carriers, etc.) and the critical information and communications infrastructure.

Third, the Ministry will help create information security clusters in areas where information security companies, convergence test beds and research institutes can collaborate seamlessly with each other to foster synergies for new markets for identify; and actively sponsor information security startups by sharing security vulnerabilities, providing test beds and supporting international certifications in a bid to lead excellent security ideas to business success.

Fourth, security will be embedded in all phases of IoT products and services from the initial concept, planning and design to implementation and verification in order to actively promote demand for IoT security by implementing IoT convergence security POC projects and to ensure the successful market entry of IoT security products by testing, verifying and commercializing them. Furthermore, the Ministry plans to actively develop security models with the aim of resolving the security issues of emerging industries, including the drone industry, and to transform them into growth drivers by encouraging the advancement of physical security industries for next-generation CCTV and biometric identification products.

② To develop original security technologies into first-movers in the global market, the Ministry plans to implement a global security technology initiative to narrow the technology gap with advanced countries and develop user-centric security technologies while expanding and strengthening joint international research to foster global technological competitiveness.

Pace-setting innovative security technologies will be developed to respond to new breeds of threats including new threats in the ICBM (IoT, Cloud, BigData, Mobile) environment, security threats to the control networks of critical infrastructures, and intelligent cyber threats (i.e. ATP attacks). The development of smart security cognitive technology will be fostered for cyber threat detection technology and forensic technology designed to locate the sources of attacks, etc. In addition, priority will be given to the development of usable security technologies that can bolster security levels and user convenience, such as fraud detection systems. Furthermore, the Cyber Security R&D Coordination Council will be formed with the remit of bolstering R&D cooperation and interaction with regard to the sharing of R&D outcomes, and of fostering joint research among the relevant ministries including the MSIP and MND, while the NIS notification system will be put in place to encourage R&D synergy in the form of technology transfer. At the same time, competent research resources in other countries will be granted wider opportunities to participate in the R&D programs of Korea, and joint international research initiatives with prestigious research labs and universities in the field of cyber security will be promoted within an open global cyber security R&D governance structure.

③ To nurture elite security resources and promote a culture of rigorous information security practice, the Ministry will work to expand the life-cycle nurturing system and education infrastructure with the aim of cultivating elite human resources who will be responsible for national cyber security, and wage a nationwide information security culture campaign to encourage the involvement of citizens, business organizations and government organizations.

New colleges specializing in information security will be opened (three by 2015) to enable promising information security talents (junior "white hat" hackers) to gain admission to the colleges of their choice, and cyber security specialty programs will be implemented as a part of the police and military service system to prevent career interruption due to the military service obligation. In addition, security coordinators will be nurtured to bolster the security capabilities of employees in the financial services and manufacturing industries, and elite security resources ("K-Shield Military" for national defense; "K-Shield Finance" for financial technologies) will be nurtured proactively in the applicable domains (2015: 1,000 specialists → 2019: 7,000 specialists).

The KISA Academy will be reformed and expanded into a convergence-type elite security talent academy (Cyber Security Talent Center), and a field-type cyber security training center (Security-GYM) will be established to bolster cyber security capabilities and align them with the needs of field operations. In addition, a talent recruitment foundation that exceeds the limitations of posed by employing people strictly on the basis of their educational/career background will be promoted, and an "excellent information security education institution accreditation system" will be introduced to raise the quality of information security education.

The Security All Wave campaign will be launched to embed information security as an integral part of our social culture and encourage citizens to practice information security rather than simply being aware of its importance. Information security supporters composed mostly of members of information security study clubs in colleges and next-generation security leaders will be organized and mandated to promote information security and improve the information security awareness campaign.

④ Investment will be expanded to improve resilience against cyber attack - ranging from incident prevention to response to/recovery from security intrusions, and the information security blanket area and divide will be eliminated by enhancing the provision of information security support for small and medium-sized enterprises.

Extensive cyber security due diligence will be conducted (2015: 400 cases → 2019: 2,000 cases) to strengthen the security of critical private sector facilities (ISP, ICT infrastructure) and public user services (cloud storage, routers, portals, etc.) and DID (Detection In-Depth) systems will be implemented to detect cyber attacks promptly and expand the scope of detection. Furthermore, 100,000 cyber traps designed to attract hackers will be put in place to bolster the response to electronic financial scams such as pharming and smishing, while the security of digital appliances such as smartphones, routers and CCTVs will be strengthened. Hotlines between the CISOs (3,000 persons) of government organizations and major business organizations (mobile carriers, portals, IDCs, etc.) will be put in place to expand the response system against cyber threats.

Regarding the critical information and communications infrastructure, protection will be beefed up along the entire supply chain covering third-party management resources, contracting, and procurement, etc., and the designation of critical infrastructures will be expanded to cover ICS (Industrial Control Systems) (400 by 2017), and proactive support will be extended to ISACs (4→7).

The proposed Nationwide 118 Information Security Support System will be implemented to provide customizable information security services for small and medium-sized enterprises and to strengthen technical/onsite support for the emergency response to and system restoration from security incidents, and more information security support centers will be established (four additional centers are due to be built in 2015). Furthermore, to narrow the information security divide between large enterprises and small and medium-sized enterprises, an information security voucher program that allows the Government to examine security vulnerabilities and subsidize a part of the response costs will be introduced in due course.

IoT
IPTV
Cloud
Big Data
LTE
Mobile
NFC
SMS

CHAPTER 4 Information Security Implementation by Sector

Section 1 Information Security in the Public Sector

1. Information Security Management Practice Assessment

The assessment of information security management practices is conducted to assess national information security policy implementation practices and thereby encourage public organizations at various levels to strengthen their in-house security management systems and promote security awareness among their employees in a bid to raise their cyber security level and assure national cyber security. The information security management practices of state/public organizations have been assessed since 2007 as per Article 3 of 「The National Intelligence Service Act」, Article 56 of 「The Electronic Government Act」, Articles 14, 21, and 22 of 「The Framework Act on Government Operation Assessment」, and Article 9 of 「The National Cyber Security Management Regulations」. In 2004, 122 organizations were assessed in that regard.

2. Establishment and Operation of a Security Command & Control Center

The Government establishes and operates security command and control centers in each sector for early detection and response to signs of cyber attacks against critical national information and communication systems with regard to government administration, energy, financial services, etc. in a bid to defend national security and interests.

No fewer than thirty-three security command and control centers have been set up at central administrative agencies around the country, which provide 24/7/365 security command and control services to protect critical data and information and communications systems from cyber attacks and share cyber threat intelligence detected and analyzed among themselves, in order to enable comprehensive and systematic responses to cyber threats at the national level.

3. Evaluation/Certification of Information Security Products

Information security products are to be evaluated and certified as per the information security system evaluation and certification standards set forth in Article 38 of 「The Framework Act on National Informatization」. In 2005, the applicable evaluation standards of the CC (Common Criteria) were unified and the applicability thereof was extended to cover all information security products in line with the trends of embedding and integrating various features into products. In 2006, Korea joined the CCRA (Common Criteria Recognition Arrangement), by which the results of evaluation and certification are mutually recognized by its members, and obtained the certificate issuer status upon entry, which helped Korean information security companies to make inroads overseas with certificates issued in Korea. Security requirements for smartphone security management products and source code security vulnerability analytics tools were developed, and the scope of evaluation/certification of products for public organizations was expanded to cover 28 types.

4. Information System Software Development Security

The Ministry of Government Administration and Home Affairs (MOGAHA) amended and publicly notified 「The Information System Implementation/Operation Guidelines for Administrative Agencies and Public Organizations」 in June 2012. These guidelines set forth software development security standards and procedures and mandatory compliance therewith. Accordingly, administrative agencies and public organizations are obligated to comply with the software development security requirements to identify and remove software security vulnerabilities during the software development phase of information projects so as to ensure software development security. To phase in compliance with the guidelines, the software development security obligation was defined to be applicable to ICT projects worth more than 2 billion won (January 2014) and to all ICT projects subject to supervision (January 2015). In August 2013, the software security vulnerability standards were amended to cover 47 project types (up from 43).

5. Secure Digital Certificate Authentication System

The digital signature governance framework is separated for public digital certificates as set forth in 「The Digital Signature Act」 and administrative digital certificates as defined in 「The Electronic Government Act」 respectively.

The administrative digital certificate system is enforced and operated as per Article 29 of 「The Electronic Government Act」. In December 2002, the system evolved into a full-blown electronic government authentication system with interface and cross authentication between private and public sector digital certificates, and the encryption key service and restoration management system was implemented in February 2006 to guarantee the continuity and security of administrative operations. To expand its penetration among public organizations and financial institutions, a public/financial authentication system was implemented in 2006, while the administrative digital certificate encryption system was further upgraded in 2011 by introducing a longer digital certificate key length (2,048 bits) and replacing the hash algorithm to guarantee the security and reliability of the administrative digital certificate. In 2012, the relevant software was upgraded to ensure the certificate's compatibility with various web browsers.

The administrative digital signature system consists of the highest-level certification authority (MOGAHA) and five certification authorities designated and publicly notified by the MOGAHA. In total, 506 registration authorities have been designated by such certification authorities to date. In addition, user authentication services are provided via a mutual interface with the public certificate system of the private sector.

As of December 2014, no fewer than 1.34 million administrative digital signatures had been issued and used in 5,654 e-government administration services available from 568 organizations. To protect personal information, a special government 'secure server' certificate (G-SSL) was adopted for the websites of administrative agencies to support the implementation of secure servers.

Following the enactment of 「The Digital Signature Act」 in February 1999, a public digital signature authentication system by which digital certificates could be issued and managed was established, with the KISA designated as the highest-level certification authority. In addition, a public certificate single-sign-on system by which one public certificate would enable e-banking transactions in all banks for greater user convenience was introduced in December 2001.

Following the designation of the Korea Information Certificate Authority Inc. and KOSCOM Co., Ltd. as the first public certification authorities in 2000, three more public certification authorities were subsequently designated.

As public certificates provide better personal information security and non-repudiation for e-transactions than traditional identification methods using the user ID and password, their application became mandatory for Internet banking (Sep. 2002) and online stock trading (Mar. 2003). In addition, in a move endorsing the security of public certificates, the Government pushed ahead with a policy to foster the use of public certificate for e-transactions and so forth, as a result of which public certificates came to be used primarily for e-finance applications such as Internet banking and online stock trading early on, although their use has since penetrated into various other domains, including web-based housing purchase applications, e-petitions, annual account settlement and tax filing, and e-procurement.

By the end of 2014, a total of 31.60 million public certificates had been issued: in particular, 28.21 million public certificates had been issued to individuals, accounting for 107% of the economically active population in Korea (i.e. 26.27 million people).

Section 2 Critical Information and Communications Infrastructure Protection

「The Act on the Protection of Information and Communications Infrastructure」 was enacted in 2001 to protect the nation's critical infrastructures. 'Information and communications infrastructure' refers to Supervisory Control and Data Acquisition (SCADA) and information communications networks relating to national security assurance, government administration, policing operations, finance, communications, transportation, and energy among others.

Facilities deemed to deserve protection from electronic intrusions among the information and communications infrastructure are designated and protected in consideration of the five criteria expressly stated in the aforementioned Act: "national/social criticality of business performed by the applicable management authority; dependence of the applicable management authority on the information and communications infrastructure for its business; mutual interface with other information and communications infrastructures; potential damage inflicted by security intrusions on national security assurance, economy and society, and the scope thereof; and possibility of security intrusion and ease of restoration/recovery therefrom.

The central administrative agency must designate the information and communications infrastructure facilities that are critical to the nation and society as critical information and communications infrastructures and manage them with priority. The management organizations thereof must analyze and assess the vulnerabilities of the critical information and communications infrastructure thus designated and implement short-, mid- and long-term protective measures to address those vulnerabilities.

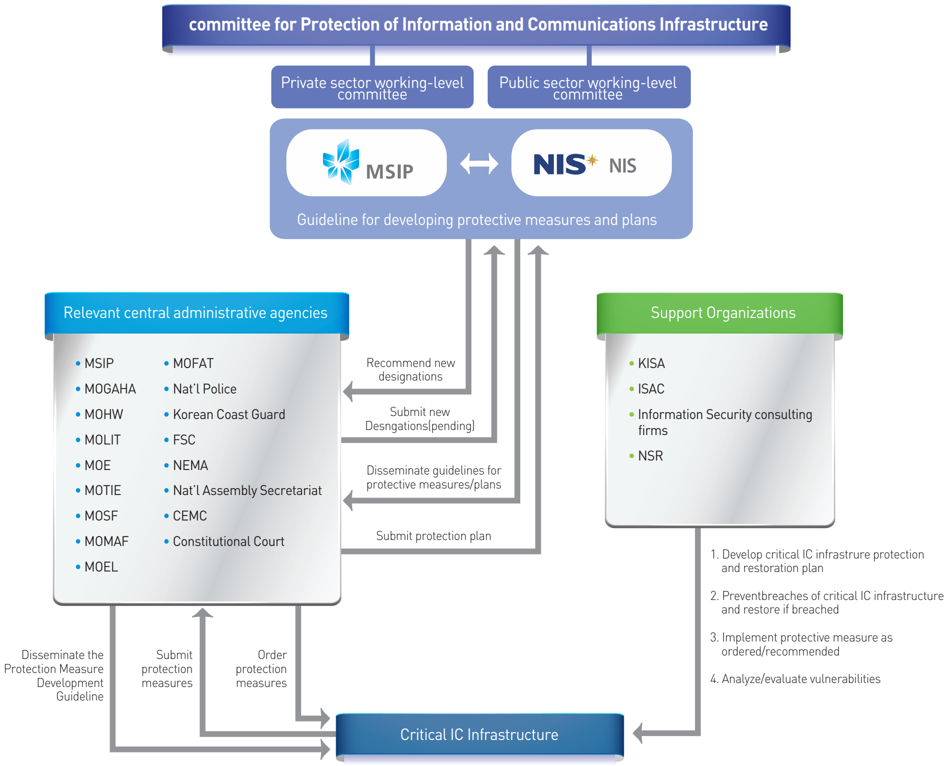
「The Act on the Protection of the Information and Communications Infrastructure」 stipulates that the Committee for the Protection of the Information and Communications Infrastructure shall be mandated to oversee and coordinate the development and implementation of the information and communications infrastructure protection policy to ensure the stable management and operation of critical information and communications infrastructures, and thereby prevent security incidents involving the relevant central administrative agency while securing synergy and collaboration in responding to security incidents.

The Committee for the Protection of Information and Communications Infrastructures is chaired by the Head of the Office for Government Policy Coordination and staffed by executives of the central administrative agency equivalent to vice ministers. The key tasks of the Committee include (1) the coordination of critical information and communications infrastructure protection policies, (2) the consolidation and coordination of critical information and communications infrastructure protection plans, and (3) deliberation on the implementation performance thereof and deliberation on key policy issues pertaining to the protection of critical information and communications infrastructures such as relevant institutional overall and new designation/revision of designation of infrastructures, etc.

Meanwhile, the Information and Communications Infrastructure Protection Working Committee supports the Committee for the Protection of Information and Communications Infrastructures to ensure its efficient operation, while the working-level committee expedites the operation of the latter Committee by reviewing and deliberating matters forwarded to or delegated from it or as instructed by its Chairman.

If the critical information and communications infrastructure is intruded upon both materially and extensively, the Headquarters for Countermeasures against Intrusion Incidents will be organized on a temporary basis under the Committee for the Protection of Information and Communications Infrastructures to handle emergency measures, extend technical support, and restore damages.

Critical Information and Communications Infrastructure Protection Governance Framework


committee for Protection of Information and Communications Infrastructure
Private sector working-level committee
Public sector working-level committee
MSIP
NIS NIS
Guideline for developing protective measures and plans
Relevant central administrative agencies
• MSIP
• MOGAHA
• MOHW
• MOLIT
• MOE
• MOTIE
• MOSF
• MOMAF
• MOEL
• MOFAT
• Nat'l Police
• Korean Coast Guard
• FSC
• NEMA
• Nat'l Assembly Secretariat
• CEMC
• Constitutional Court
Recommend new designations
Submit new Desngations(pending)
Disseminate guidelines for protective measures/plans
Submit protection plan
Support Organizations
• KISA
• ISAC
• Information Security consulting firms
• NSR
1. Develop critical IC infrastrure protection and restoration plan
2. Preventbreaches of critical IC infrastructure and restore if breached
3. Implement protective measure as ordered/recommended
4. Analyze/evaluate vulnerabilities
Disseminate the Protection Measure Development Guideline
Submit protection measures
Order protection measures
Critical IC Infrastructure

[Courtesy: Information & Communications Infrastructure Protection Guide, KISA (2014)]

The relevant central administrative agency designates the critical information and communications infrastructure, reviews the critical information and communications infrastructure protection measures submitted by management organizations, and develops and implements protection plans.

The management organizations having primary responsibility for protecting critical information and communications infrastructures analyze and evaluate the vulnerabilities of the applicable infrastructures to prevent and respond to security intrusions and develop the necessary protection measures. Further, in the event of an incident, they must notify the relevant administrative agencies, investigation authorities, or KISA of the details and take all necessary measures to contain the damages caused by the security incident and expedite the response thereto.

The support organizations include the KISA, NSR, ISAC, and information security consulting firms. The heads of the applicable management authority may call for technical support in connection with the development of critical information and communications infrastructure protection measures and the prevention and restoration of/recovery from security intrusions. The NIS and the MSIP may develop critical information and communications infrastructure protection planning guidelines and notify the heads of the relevant central administrative agency thereof.

The ex-post management arrangement has been strengthened, allowing the MSIP to verify compliance with the protection measures developed by the management organizations since 2007 in connection with the amendment of 「The Act on the Protection of Information and Communications Infrastructures」. The NIS director was given the responsibility for verifying and examining required details submitted for public facilities and the MND for national defense facilities. The MSIP was given jurisdiction over civilian facilities.

In 2014, detailed designation standards and procedural guidelines for determining eligibility for designation as a critical information and communications infrastructure as per 「The Act on the Protection of Information and Communications Infrastructure」 were developed and disseminated to secure objectivity. Based on this, the operational status and information security management practices of each facility were inspected to determine the viability of the facilities subject to their designation as critical infrastructures. For facilities identified in such inspection, it was recommended that the central administrative agency designate the reviewed facilities. As a consequence, 62 critical information and communications infrastructure facilities were newly designated, as reviewed and determined by the Committee for the Protection of Information and Communications Infrastructures.

Critical information and communications infrastructures began to be designated following the enforcement of 「The Act on the Protection of Information and Communications Infrastructure」 in July 2001, and, as of December, 2014, 17 relevant central administrative agencies, 188 management organizations, and 292 infrastructure facilities had been designated and managed in the fields of information & communications, media, financial services, transportation, energy, nuclear power, water supply, food & drug management, health & welfare, government sector, social security facilities, construction & management, geographic information, and others.

Section 3 Information Security in the Private Sector

1. Operation of the Korea Internet Security Center

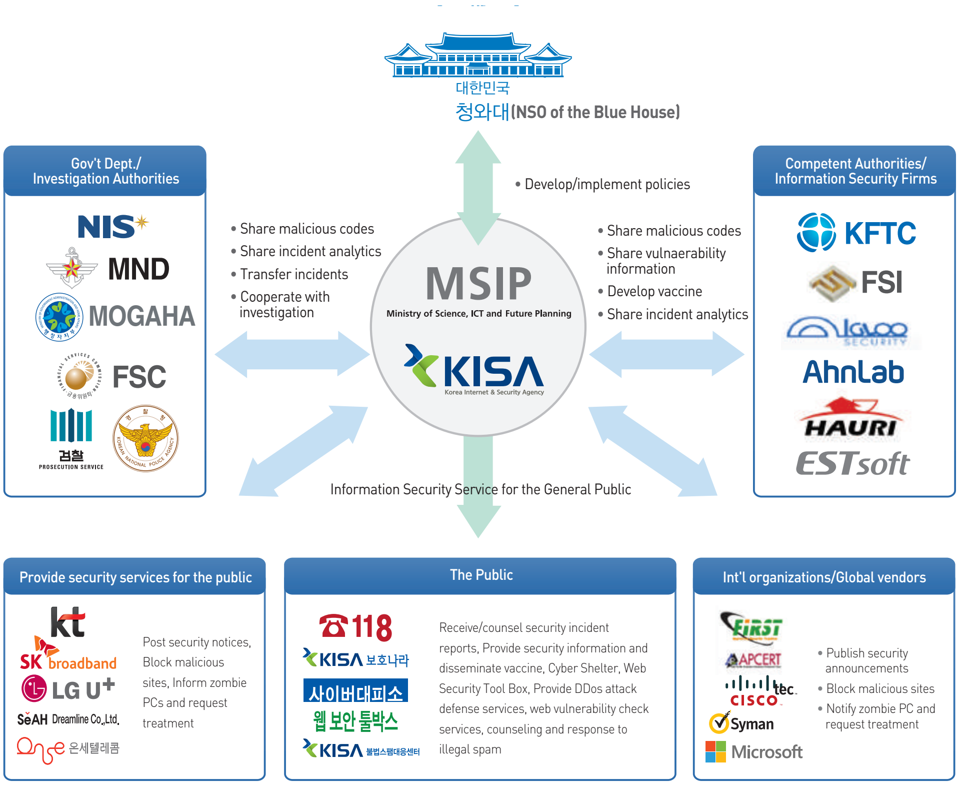
The KISA performs a variety of activities including operation of the Korea Internet Security Center (KISC).

The KISC at KISA is now operated on a 24/7/365 basis to monitor suspicious activities on the Internet, initiate counter-responses to intrusion incidents, and provide a communication channel for joint response, etc.

The KISC (1) constantly monitors domestic traffic on the Internet, major DNS services, and key web servers connecting the government, public and financial sectors, (2) receives reports of and provides initial responses to DDoS attacks, phishing incidents and website hacking attempts, and (3) evaluates the risks posed by new malicious codes and security vulnerabilities in order to align counter-responses commensurate to the risk level.

The KISC provides a communication channel for sharing information and coordinating responses with the competent authorities in Korea and the rest of the world, and kicks into action the emergency response system whenever high-profile political or social issues arise. The cooperation framework is tightly maintained with the leading information and communications service providers, security service providers and competent authorities. Workshops are held semi-annually to promote information sharing on key pending issues of information security and to facilitate the exchange of information on matters calling for mutual cooperation. Furthermore, joint mock exercises are conducted with the competent authorities in Korea and the rest of the world to enable a prompt and efficient response to information security incidents.

Information Security Governance Framework in the Private Sector



Gov't Dept./ Investigation Authorities

Competent Authorities/ Information Security Firms

- Develop/implement policies

- Share malicious codes
- Share incident analytics
- Transfer incidents
- Cooperate with investigation

- Share malicious codes
- Share vulnaerability information
- Develop vaccine
- Share incident analytics

Information Security Service for the General Public

Provide security services for the public

Post security notices, Block malicious sites, Inform zombie PCs and request treatment

The Public

Receive/counsel security incident reports, Provide security information and disseminate vaccine, Cyber Shelter, Web Security Tool Box, Provide DDos attack defense services, web vulnerability check services, counseling and response to illegal spam

Int'l organizations/Global vendors

- Publish security announcements
- Block malicious sites
- Notify zombie PC and request treatment

2. Detection of and Response to Websites Hosting Malicious Codes

The KISA has searched some 2.6 million Korean Web domains to protect domestic Internet users from infection with malicious codes by accessing web pages hosting them, detecting and thwarting 47,703 malicious codes accordingly. In 2013, a system dedicated to the inspection of cloud-hosted exclusive-use programs was established and operated, while in 2014 the main pages of major websites were scanned dynamically for potential infection with malicious codes.

3. Response to DDoS Attack & Zombie PCs

The KISA has installed and is now operating a DDoS response system that detects and responds to DDoS attacks early in the Internet interface section, which is a node of Internet traffic exchange among ISPs, and also monitors any signs of imminent attack. As of 2014, DDoS response systems were being operated by 12 ISPs, covering 20 interface sections. During the past six years, a total of 1,772 DDoS attacks in the interface sections have been detected and thwarted, including 457 DDoS attacks in 2014. Following the detection of these DDoS attacks, a zombie PC IP list was secured, malicious code treatment encouraged, and immediate response requested to the ISPs and site administrators in a bid to minimize the proliferation of damage from DDoS attacks.

The DDoS cyber shelter service, which is designed to detour attacking traffic away from targeted websites and allow ordinary users to use such websites as intended, is provided to minimize potential damage to small and medium-sized enterprises that are less capable of coping with DDoS attacks on their own. Since the launch of this service in 2010, 1,001 organizations have used the service (as of 2014), and the DDoS defense service has been provided in 449 cases of attack. As the anti-DDoS defense was provided in combination with the treatment of zombie PCs and the block of servers from which attack commands originated, the recurrence of infections by malicious code has also been prevented.

The cyber curing service for zombie PCs notifies the users of zombie PCs that their PCs have been infected, and offers them customized vaccines to treat the PCs more systematically. To ensure users keep abreast of infections intuitively, infection notices pop up whenever a zombie PC user connects to the Internet via his or her web browser, and a customized vaccine designed to cure zombie PCs of the relevant malware is also provided together to facilitate the cure.

The infection notification and curing system, which was expanded and implemented in cooperation with ISPs including KT, SK Broadband and T-Broad in 2010, and expanded further to include LG U+, CJ Hello Vision, C&M, and Hyundai HCN in 2013, now covers most Internet users in Korea. In addition, the scope of the service was extended to include three more small SOs (service operators) in 2014 to allow even more PC users to access the treatment service. In addition, a mobile emergency cyber curing system capable of notifying and curing smartphones infected with malicious mobile apps has been implemented on a trial basis, with full-scope deployment to all smartphones planned for 2015.

Since its launch in January 2011, the zombie PC cyber curing system has published 151 cure announcements, sent infection notices to 248,281 zombie PCs, and produced and distributed 67 customized vaccines in 2014.

4. Responses to Internet Security Incidents

The KISC and KrCERT/CC plays a leading role in responding to security intrusions by joining international security intrusion response councils such as FIRST or APCERT, and proactively participates in cyber security discussions in the international community. In addition, KrCERT/CC provides training programs to developing countries to enable them to cope with information security intrusions more effectively.

Since 2004 a joint public-private sector "expert pool" has been in operation pursuant to Article 48.4 of 「The Act on the Promotion of Information and Communications Network Utilization and Information Protection, etc.」 with the remit of providing countermeasures to prevent the proliferation of damage, responding to security intrusions, performing the necessary restoration, and preventing the recurrence of critical security intrusions into information and communications networks. However, as the public-private sector joint investigation team is organized on an ad-hoc basis pursuant to the applicable legal and regulatory provisions in the wake of critical security intrusions, a cyber security specialist group has been mandated to conduct cyber security intrusion prevention campaigns and ensure that a prompt response is organized and operated at normal times.

5. ISMS Certification

The Information Security Management System (ISMS) stipulates that a chief information security officer shall be appointed to align information security with the business management policies of business organizations and to analyze the risks to information assets so as to provide inputs to information security policies and consequently initiate information security activities. In addition, the ISMS requires that information security activities that are performed in accordance with information security policies be monitored and reviewed for continuous improvement.

The ISMS certification system is designed to provide standards for activities aimed at protecting information assets from various threats to ensure the security and continuity of the information and communications services of an organization in accordance with Article 47 of 「The Act on the Promotion of Information and Communications Network Utilization and Information Protection, etc.」. The system assesses whether the information security activities of a given organization comply with the ISMS certification standards and issues the certification accordingly. The certification standards consist of an information security management processes involving the participation of the management along with stronger responsibility (12 mandatory control items) and information security measures (92 optional control items).

As of December 2014, a total of 482 ISMS certificates (cumulative terms) had been issued since the first issuance thereof in 2002, and 377 certificates issued to date are now maintained. All business organizations and other institutes implementing and operating the ISMS are allowed to apply for ISMS certification and receive the certificate, subject to the results of certification review and deliberation by the certification commission. However, electric communications service providers and information and communications service providers that can have a significant impact on the security of information and communications networks are designated as compulsory subjects pursuant to Article 47.2 of 『The Act on the Promotion of Information and Communications Network Utilization and Information Protection, etc.』. Entities subject to the ISMS certification are divided into voluntary applicants and mandatory subjects, and entities that are subject to mandatory ISMS certification as provided for in the applicable laws must receive ISMS certification every year.

6. Preliminary Information Security Inspection

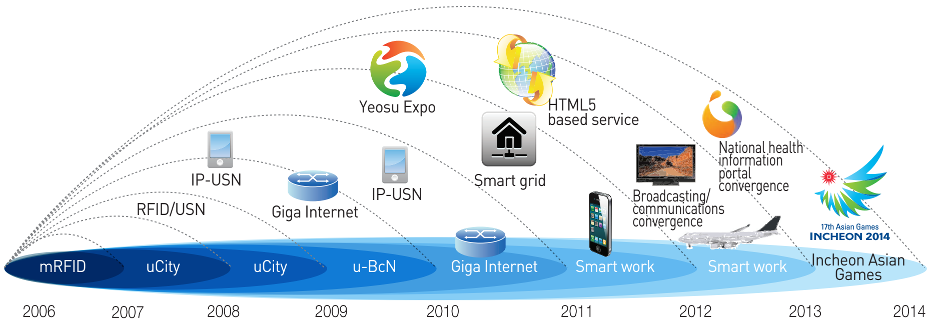
「The Act on the Promotion of Information and Communications Network Utilization and Information Protection, etc.」, which provides for recommendations concerning security measures to be established from the service planning or design phase, was added in February 2012 and took effect on February 18, 2013.

The preliminary information security inspection is a process by which information security threats, vulnerabilities and risks are analyzed when new information and communications infrastructures or services are planned so as to be able to implement and deliver services that are free from potential security threats.

The preliminary information security inspection includes 78 specific inspection items in 54 categories in six phases. The phases of the preliminary information security inspection are aligned with generic software implementation phases. Each phase consists of specific information security inspection items and can be performed independently.

Drawbacks that could leave confidential information vulnerable to wiretapping during video conferences were identified in the smart work pilot project performed in 2011; vulnerabilities that could lead to aviation accidents by allowing false aviation control signals to mislead airplane pilots were found in the aviation control system development project performed in 2012; and administrator page access control loopholes were found in the 2013 Incheon Asian Indoor and Martial Arts Games. All in

KISA Performs Preliminary Information Security Inspection



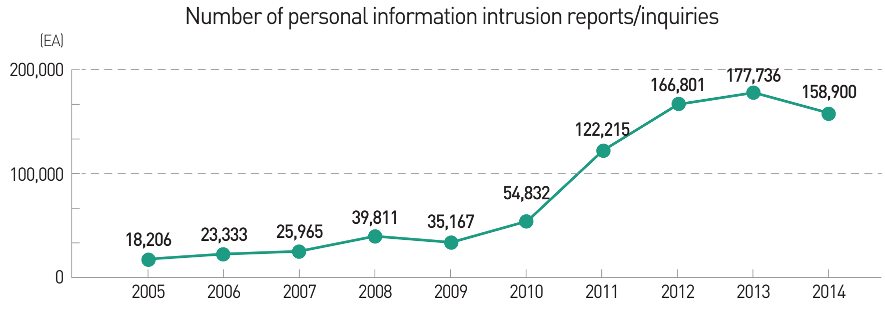
all, more than 3,000 security vulnerabilities have been identified and removed since 2006, thus making a significant contribution to the security and reliability of information and communications services.

The KISA performed preliminary information security inspections on many national infrastructure projects including the information system project for the 2014 Incheon Asian Games, and will perform the same inspections for the disaster communications network project and the 2018 Pyongchang Winter Olympic Games information system, etc.

Section 4 Personal Information Protection

In 2014, no fewer than 158,900 cases of personal information incidents were received by the Personal Information Intrusion Report Center of the KISA, including reports of personal information intrusions, inquiries and applications for remedies against information intrusions, which was about 19,000 fewer (or 12% less) cases than the 177,736 cases recorded in the previous year. Interestingly, one of the reasons why the

Personal Information Intrusion Reports/Inquiries Received per Year (In: 1ea.)



[Courtesy : KISA, 2015.1]

number of cases decreased in comparison with the year 2013 was that, in the wake of the enforcement of legal

requirements in the amendment to 「The Personal Information Protection Act」 in August 2014, most of the relevant inquiries and civil complaints were directed to the Resident Registration Number Clearance Center, which reduced the number of cases reported to the Personal Information Intrusion Report Center.

In fact, the number of personal information reports and inquiries concerning disclosure, intrusion or abuse involving a third party's information, including resident registration numbers, came to 83,126 (52.31%) in 2014, which was down by more than 55% from the 129,103 cases recorded in the previous year, whereas the number of reports and inquiries relating to unauthorized personal information collection came to 3,923, and the number concerning a lack of technical or managerial measures came to 7,404, showing an increase of 33% and 40%, respectively, over the previous year.

The number of cases of unauthorized disclosure of credit information to third parties governed by 「The Act on the Promotion of Information and Communications Network Utilization and Information Protection, etc.」 and 「The Personal Information Protection Act」 came to 57,705, accounting for the second largest share next to cases relating to leakage or abuse of resident registration numbers. There is a prevailing trend whereby personal information intrusion reports/inquiries span increasingly diverse and specific areas such as healthcare, finance, education and welfare.

Section 5 Information Security Campaign

The '118' Hotline is a one-stop service that answers the grievances and inquiries of citizens concerning various topics related to Internet use including hacking, computer viruses, personal information intrusion, spam, online authentication, and domain names, etc. Citizens can access the help desk service free of charge simply by dialing 118 anywhere anytime.

Information Security BI

In 2014 about 630,000 calls were made to 118, up about 3.5% from the 610,000 calls made in 2013. The topics discussed were in the order of the Internet in general, personal information, hacking/viruses, and spam. Interestingly, the number of calls made about hacking/viruses and spam in 2014 increased YoY by about 28%. In 2014, there were 153,000 such calls compared to the 119,000 calls made in 2013. This was primarily attributable to the prevalence of financial fraud smishing and pharming targeted at smartphones.

The information security BI “Jiki-GO! Nuri-GO!” was devised for the information security promotion campaign. The arrow and stop sign in "Jiki-Go" are designed to suggest to users that they take a pause and think before accessing the Internet, whereas the smile in "Nuri-Go" symbolizes a wholesome and happy Internet life.

The annual “Jiki-GO! Nuri-GO!” campaign held diverse online SNS events to promote information security guidelines relevant to the daily routines of individual citizens, followed by a variety of offline campaigns designed to foster information security in person through direct communication with the general public. In addition, an information security testimony contest, slogan contest and illustration contest were held in the second half of 2014 to enable citizens to engage directly in information security activities, and an information security calendar using the winning entries of those contests was published and distributed to the public in 2015.

IoT
IPTV
Cloud
Big
Data
LTE
NFC
Mobile
SMS

CHAPTER 5

Creation of Foundation for Information Security

Section 1 Fostering of Information Security Industry

Information security companies in Korea have world-class technical prowess and competitiveness in their business domain and have grown significantly to the extent of supporting the information security needs of Korea adequately.

Network security (KRW 473.4 billion) and contents/information leakage prevention security (KRW 268.7 billion) accounted for a significant share of the information security market, and demand for products relating to such domains increased dramatically in the wake of the recent personal information intrusion incidents. In terms of information security service, security consulting services increased significantly as attacks became more intelligent, advanced, complex and diverse, calling for a more fortified maintenance and information security maintenance system.

In terms of the physical security market, security patrol services (KRW 1.293 trillion) and CCTVs (KRW 1.1943 trillion) accounted for the most significant market share, with access control (15.7%), peripheral devices (13.2%) and IP imaging devices (9.3%) all growing significantly. In terms of physical security services, security patrol services (8.2%) grew remarkably, while the networking of physical security products, vehicle black boxes, and new services (home and infant monitoring service, etc.) emerged as major issues.

In terms of information security revenues by (customer) sector in 2014, the public sector accounted for the highest portion at 34.2%, followed by the service sector at 25.1%, the manufacturing sector at 21.1%, and the financial services sector at 19.7%.

The information security consulting firm designation system designates private firms recognized for their professional prowess and reliability as information security consultants with the capability to analyze vulnerabilities in the critical information and communications infrastructure and to provide consultation on protective measures in a bid to ensure the delivery of quality information security services. This system has been enforced as per 「The Act on the Protection of Information and Communications Infrastructure」 and 「The Information and Communications Industry Promotion Ac」. The applicable designation standards, procedures, methods and other details thereof are set forth in 「The Public Notification on the Designation of Information Security Consulting Firms, etc.」. So far, 18 firms have been designated as information security consulting firms.

In April 2010, 『The National Cyber Security Management Regulation』 provided for a mandatory obligation for state/public authorities to establish security control centers. In a sequel to the regulation, 「The Public Announcement for Designation of Security Control Contractors, etc.」 was released in June 2013 to designate contractors mandated to run the security control sectors effectively.

The security control contractor designation system was enforced from July 1, 2011 with the designation of twelve contractors in the first batch on October 31 of the same year. However, in the follow-up review of 2012, two of those designations were revoked, and the contractors in question were replaced with two new contractors. In the follow-up review of 2014, one designation was revoked, so currently there are eleven contractors who have been designated as security control contractors.

With the mandatory obligation for security control of state/public organizations and the enforcement of the security control contractor designation system, the revenues of security control services for state/public organizations increased to about KRW 57.3 billion, with the total expected to increase to KRW 75.4 billion by 2018.

Section 2 Development of Information Security Technology

To identify and develop world-class information security products, applicable markets and technologies are analyzed and core technologies identified based on feedback from experts. To that end, thirty-four information security product categories were analyzed in consideration of cyber threats and the volume of the domestic information security market, etc. with the following strategic product categories identified.

Core Information Security Technology Development Domains

Market Volume	KRW 10B~40B	KRW 40B~70B	KRW 70B~90B	KRW Over 90B
⟨As-is security threats⟩ Worm·virus, unauthorized access, DDoS, unsolicited spam, web hacking	PC firewalls, anti-spyware, spam blocking, security operation system, SSO (single-sign-on), DDoS response	Firewalls, web firewalls, VPN, public/private authentication services, integrated security management PKI	DB security (access control), PC security, DRM Intrusion prevention, virus vaccine, security control	DVR, CCTV, video engine/chipset
⟨Emerging security threats⟩ Wireless/mobile threat, intelligent attack (APT), cyber scam, intrusion of personal/enterprise data, threat to social security	Vulnerability analytics tools, log management analytics tools, wireless network security, mobile security, secure USB, secure smart card, iris recognition harmful contents blocking	DB password, face recognition	Video monitoring management, video monitoring intelligent solutions, social infrastructure protection	–
10 strategic products	(Intelligent threat) response to malware (intrusion prevention+virus vaccine+vulnerability analytics tool), security control (security control+log management analytics tool) (High growth rate) wireless security, smart device security (mobile security+secure smart card), social infrastructure protection (Social security) video monitoring (video monitoring management+video monitoring intelligent solution), biometrics (face+iris recognition), contents security (Personal information protection) next-generation password (DB password), smart authentication (secure USB+PKI)			

Anti-malware and security products were selected as product groups requiring technological evolution to respond to intelligent cyber threats; and wireless security, smart device security and social infrastructure protection products were selected as product groups associated with ever-rising growth rates in the wake of changes in the wireless and mobile information and communications technology environment. In addition, video monitoring, biometrics and contents security products were selected as product groups that can contribute to social security by preventing the propagation of crime and illegal/hazardous information, whereas next-generation password and smart authentication products were selected as product groups with the capacity to support responses to threats to personal information in a variety of connection environments including big data, cloud, etc.

The ten strategic information security product groups selected above were reclassified into three types - import substitution, export driver, and future growth types - in consideration of the market share of local products, export volume, and the potential for future markets, etc. Import substitution products are a product group in which there are few homegrown products in the domestic market (the market share of homegrown products is around 12% or less) and where global competitor products are likely to make inroads into the domestic market, necessitating defense of the domestic market. Mobile security, smart device security, and social infrastructure protection products belong to this product group. Export driver products are a product group in which homegrown products dominate the domestic market, but their global competitiveness is not strong enough (their export volume accounts for only 6% of domestic revenue). Anti-malware, security control, video monitoring, biometrics, and contents security products belong to this category. Lastly, future growth products are a product group in which products are selected as promising/original technologies that, if developed ahead of others, could result in leadership in the global emerging markets. Next-generation password and smart authentication belong to this category.

1. Development of Original Information Security Technology

In 2014, twenty-six national R&D projects were conducted by many business organizations and research institutes in the field of information security. The current status of information security technology development including major original technologies likely to affect domestic information security technology is as follows:

A. Cyber blackbox and integrated cyber security situation analytics technologies

Cyber blackbox technology is designed to store volatile network traffic data for a long time and ensure the integrity thereof, so to enable prompt analysis of and response to the causes of security intrusions in a bid to facilitate a response before and after an advanced cyber attack. In addition, integrated cyber security analytical technologies based on blackbox technologies support the tracking of attackers and the forecasting of attacks through correlation analysis and profiling techniques using massive intrusioned data

B. Script-based cyber attack prevention and response technology

Script-based cyber attack prevention and response technology is designed to detect and block attack attempts through in-depth script analytics and to verify malicious script distribution servers and script integrity in advance so as to detect/block script-based web attack attempts that are hard to detect with conventional security equipment.

C. 4G mobile communications network attack and abnormal traffic detection/response technology

Generation 4 mobile communications network (aka "4G network") attack and abnormal traffic detection/response technology is designed to detect and block attacks likely to cause failure of mobile data and voice services such as DDoS (Distributed Denial of Service) attacks. It is an original technology suitable for protection of the mobile communications network infrastructure.

D. Privacy-enhanced personal information distribution security core technology

Privacy-enhanced personal information distribution security core technology is a list/negotiation-based security curation technology that allows users to receive secure and convenient smart services from various entities in smart environments.

E. Large-volume data analytics-based cyber attack target recognition and tracking technology

Large-volume data analytics-based cyber attack target recognition and tracking technology detects intelligent cyber attacks and targets in advance based on long-term historical analysis of intranet multi-source data in order to secure mission-critical information systems. In addition, cyber target tracking technology is used to respond to attacks preemptively by tracking distribution sites and attacks originating from infection sites that attempt targeted enterprise attacks.

2. Development of Commercial Information Security Technology

Among information security companies in Korea, 87 (63.5%) operate in-house technology development research institutes and 14 (10.2%) run a dedicated department, which indicates that many of them are trying to develop homegrown technologies. In addition, among the 87 companies operating in-house research labs, 37 of them employ 10~50 persons, 20 employ 50~100 persons, and 27 employ more than 100 persons. Among those which do not operate research labs, companies employing 10 to 50 persons account for the majority at 22, while there are 9 companies employing fewer than 10 persons. A total of 82 companies invested in R&D in 2014, with their average R&D investment amounting to KRW 1.572 billion. Average investment in technology introduction amounted to KRW 209.4 million, and average investment in the various certification programs of 43 companies came to KRW 107.6 million.

Section 3 Education on Information Security

1. Information Security Industry and Education

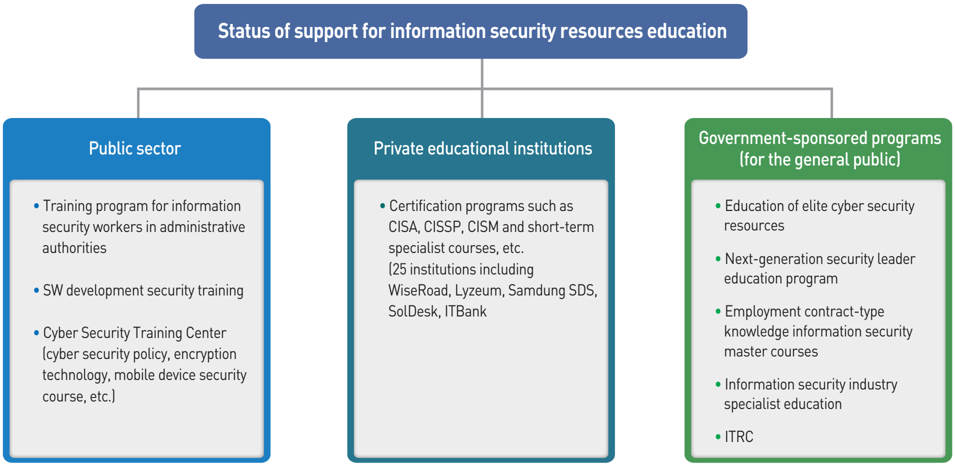
In 2014, a total of 109,508 people were working in 653 companies based in the information security industry, of whom 36,258 were working in information security jobs. In terms of resource breakdown by competency level, beginners accounted for 14,752 (40.7%), intermediate level workers for 8,810 (24.3%), senior level workers for 7,366 (20.3%), and specialist level workers for 5,330 (14.7%).

In terms of breakdown of information security resources by technical competency, beginner level resources responsible for information system management accounted for the majority at 724 persons in the field of information security, whereas senior level resources in charge of application software were the majority at 1,007 persons in the physical security domain, excluding management and other jobs.

According to a survey, 76 information security-related departments were open in 2014, with 8 in technical colleges, 36 at universities and 32 at graduate schools. Some 7,510 students are now registered in those departments, and 826 information security majors graduated from regular educational institutions in 2014, with 110 from technical colleges, 435 from universities, and 281 from graduate schools.

Information security resource education is supported by both the public and private sectors, and by government-sponsored programs, depending on the subjects taught. In the public sector, cyber intrusion response and software development security training classes are available all year around for the information security workers of administrative authorities and their affiliated organizations. In addition, annual training programs are offered by the cyber security training center, etc. to produce cyber security resources skilled in real-life attack and defense. Meanwhile, private educational institutions also provide various information security professional programs such as information security qualification certificate programs and short/long-term specialist courses in reflection of the rising demand for information security education. Furthermore, the Ministry of Science, ICT and Future Planning provides senior information security resource training programs in partnership with the KISA and the National IT Industry Promotion Agency, etc.

Information security resource education framework



Status of support for information security resources education

Public sector

- Training program for information security workers in administrative authorities
- SW development security training
- Cyber Security Training Center (cyber security policy, encryption technology, mobile device security course, etc.)

Private educational institutions

- Certification programs such as CISA, CISSP, CISM and short-term specialist courses, etc. (25 institutions including WiseRoad, Lyzeum, Samdung SDS, SolDesk, ITBank

Government-sponsored programs (for the general public)

- Education of elite cyber security resources
- Next-generation security leader education program
- Employment contract-type knowledge information security master courses
- Information security industry specialist education
- ITRC

2. Hacking Defense Contests

The Government and other relevant institutions and organizations hold various events such as hacking defense contests in a bid to identify and nurture information security professionals and improve awareness of information security, with the following major events held in Korea in 2014.

A. Korea White Hat Contest

The Korea White Hat Contest was held to identify and nurture cyber security talents in Korea. Unlike other hacking defense contests, this one was run in two separate categories - a junior division and an adult division. A total of 827 contestants took part in the contest, including 327 persons of 161 teams in the junior division and 500 persons of 228 teams in the adult division. After the qualifying round, 8 teams from the junior division and another 8 teams from the group division made it to the final stage, respectively.

B. HDCON

Launched in 2004, the HDCON (Hacking Defense Contest) is the longest-running anti-hacking contest held in Korea. Focusing on incident analysis and defense rather than attack, this contest is organized by the MISP and managed by the KISA, with the 11th contest held in 2014. A total of 501 teams joined the qualifying round, of which 10 made it to the finals. Interestingly, the 2014 HDCON, rather than adopting the conventional problem-solving approach, opted for the simulation of an actual security intrusion case on a virtual network.

C. CODEGATE

CODEGATE, initiated in 2008, was the first international hacking defense contest ever hosted in Korea. In 2014, 1,200 teams from 74 countries competed, of which 12 made it to the finals after a qualifying round. In the finals the 12 teams vied with three other international contest winners who joined the event on invitation.

D. SECUINSIDE

SECUINSIDE is designed to raise awareness of e-finance information security. The 4th SECUINSIDE, held in 2014, was joined by 940 teams from 94 countries, of which 10 made it to the finals. In the final round the contestants were presented with problems relating to the vulnerabilities of financial IT.

3. Information Security Qualification Program

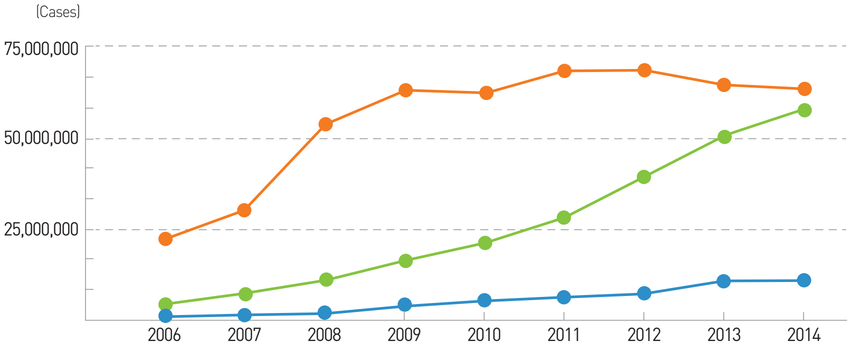
As information security becomes ever more critical and demand for the relevant resources increases accordingly, interest in information security professional qualification programs as a means of evidencing theoretical and practical information security skills is mounting progressively.

Information Security Professional Qualifications

Category	Name	Class	Managing Authority
Domestic	Information security engineer/ industrial engineer	-	Ministry of Science, ICT and Future Planning, KISA
	Digital forensic expert	Class 1, Class 2	Korea Forensics Society, KISA
	Internet security expert	Class 1, Class 2	Korea Information and Communications Certification Association
	Information security manager(ISM)	-	Korea Information Assessment Association
	Hacking security expert	Class 1, Class 2, Class 3, Junior	Korea Hacking Defense Association
Global	Certified information system security professional (CISSP) Certified cyber forensic professional (CCFP)	-	ISC2
	Certified information security manager (CISM)	-	ISACA

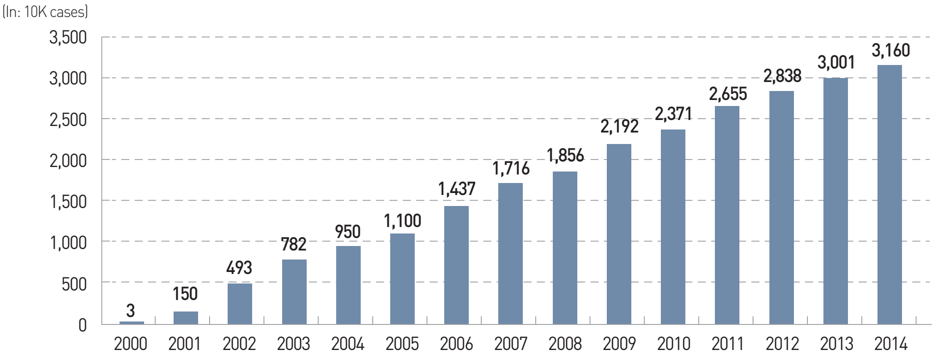
Appendix

Government Helpdesk Portal Minwon 24 Service Status



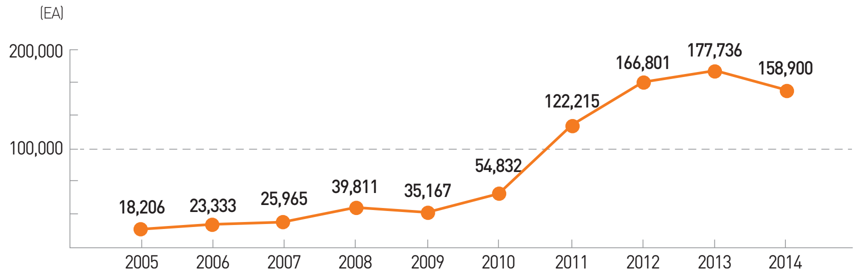
[Source: Ministry of Government Administration and Home Affairs (Government civil complaint portal Minwon24)]

Trend of Public Certificate Users by Year



[Source: Korea Internet & Security Agency]

Personal Information Intrusion Reports/Inquiries per Year (In: 1ea.)



[Source: Korea Internet and Security Agency, 2015.1]

Personal Information Intrusion Reports and Inquiries (In: 1ea. / %)

Type	2013		2014	
	No. of Cases	%	No. of Cases	%
Collection of personal information without user's consent	2,634	1.48	3,923	2.47
Personal information collection notices/statements	84	0.05	268	0.17
Excessive collection of personal information	1,139	0.64	1,200	0.76
Unauthorized use or third-party disclosure	1,988	1.12	2,242	1.41
Abuse/intrusion by personal information handler	1,022	0.58	1,036	0.65
Personal information handling outsourcing notice obligation	44	0.02	40	0.03
Business assignment notice obligations	47	0.03	54	0.03
Personal information management supervisor	51	0.03	39	0.02
Lack of technical/managerial measures	4,518	2.54	7,404	4.66
Failure to scrap personal information following fulfillment of agreed purpose	602	0.34	686	0.43
Withdrawal of consent, request for access or correction	674	0.38	792	0.50
Withdrawal of consent, requests for access or correction to be made easier than collection	510	0.29	352	0.22
Collection of children's personal information	36	0.02	33	0.02
Abuse, intrusion, theft of third-party information such as resident registration number	129,103	72.64	83,126	52.31
Violation of 'The Act on Promotion of Information and Communications Network Utilization and nformation Protection' and 'The Personal Information Protection Act' (inquiries relating to credit information, etc.)	35,284	19.85	57,705	36.32
Total	177,736	100	158,900	100

[Source: Korea Internet and Security Agency, Jan. 2015]

☎118 Counseling by Category (In: 1ea.)

Classification	Personal information	Spam	Hacking/ Virus	Domain/IP	Internet in general	Total
2014	155,908	134,297	153,046	2,519	187,990	633,760
2013	175,389	105,395	119,247	3,191	209,274	612,496
2012	164,698	112,482	57,710	1,856	140,646	477,392

※'Internet in general' means counseling type for inquiries concerning issues arising in using the Internet or a communications device, guidance on the competent authority, etc.

[Source: Korea Internet and Security Agency]

Status of Employment by Information Security Companies (In: 1ea. / %)

Classification	Information Security		Information Security		Total	
	No. of companies	%	No. of companies	%	No. of companies	%
Fewer than 10	71	27.7	104	26.2	175	26.8
10~49	113	44.1	207	52.1	320	49.0
50~100	29	11.3	36	9.1	65	10.0
More than 100	43	16.8	50	12.6	93	14.2
Total	256	100	397	100.0	653	100.0

[Source: 2014 Korea Information Security Industry Survey, Information Security Industry Association]

Product and Service Revenue of Information Security Companies (In: 1M KRW / %)

Classification		2013	2014	Growth Rate
Information security products	Network security	448,224	473,412	5.6
	System security	212,982	215,484	1.2
	Contents/information leakage prevention	257,716	268,782	4.3
	Encryption/authentication	126,761	126,792	0.0
	Security management	97,542	111,350	14.2
	Other products	133,316	124,691	-6.5
	Subtotal	1,276,541	1,320,511	3.4
Information security services	Security consulting	76,061	82,279	8.2
	Maintenance	85,212	90,776	6.5
	Security control	150,310	157,892	5.0
	Education/training	16	15	-6.3
	Certification service	42,973	44,282	3.0
	Sub-total	354,572	375,244	5.8
Total		1,631,113	1,695,755	4.0

[Source: 2014 Korea Information Security Industry Survey, Information Security Industry Association]

Korea Internet & security Agency

KISA Korea Internet & Security Agency

The KISA has set 'Internet promotion for the future' and 'information security for our safety' as its two primary tasks, and is focusing on enhancing the information security capacity of Korea's ICT industry and expanding global cooperative partnerships based on the K-ICT Security Development Strategy, to ensure that these two pillars will serve as the core competencies of the future Korea in an equal and harmoniously balanced manner.

Protecting the industry from the risk of cyber attack and preventing privacy infringement

- Operation of the Korea Internet Security Center and KrCERT/CC
  - Monitoring of cyber threats such as DDoS attacks and distribution of malicious codes on a 24/7/365 basis.
  - Operation of the DDoS Response System (DDos Cyber Shelter Service).
  - Detection of and response to Websites hosting malicious codes.

    * The KISA has searched the 2.5 million Korean domains to prevent local Internet users from infection with malicious codes by accessing web pages that host them.
- Research & Development of Information Security Technology
- Information Security Management System (ISMS) Certification
- Education of elite cyber security experts (KISA ACADEMY)
- Operation of the Personal Infringement Report Center and the Illegal Spam Response Center

Promoting the Internet and Information Security Industries

- Evaluation and certification system for information security products (CCRA)
- Support Center for the IPv6
- Korea Domain Name System (KrDNS)
- Korea National Biometric Test Center
- Regional information security bases
- IoT Innovation Center
- 'Born-Global Project' and Internet Startup (K-Global Startup)

Expanding International Cooperation and Business Overseas

- Global cooperation network with ITU, OECD, World Bank, FIRST, APCERT, ICANN, APNIC, etc.
- Initiation of a new global cooperation platform named CAMP

  * CAMP : Cybersecurity Alliance for Mutual Progress
- A total of 33 MoUs signed with foreign counterparts (as of June)

Cybersecurity Alliance for Mutual Progress

Global cooperation to ensure a safer cyber environment

The borderless characteristic of cyber threats is certain to create new challenges ahead. It is now imperative to respond to such threats in a collective and collaborative manner to secure a safe global cyberspace. In an effort to raise cooperation and knowledge sharing to a higher level, the KISA has initiated a partnership program to gather and share its experiences with other nations and organizations.

Solidifying common ground for a safer cyberspace

Ensuring global cyber security is crucial to underpinning growth and innovation in the online environment and the wider digital economy, and to supporting human well-being, human rights and prosperity for all.

Unifying sporadic isolated efforts into a coordinated global platform

As the scale of cyber-threats has evolved from the national- to the global-level, it is necessary to work with each other and martial our efforts to countervail such malicious intents on the global stage.

Enhancing the cyber capability of member countries

In order to equip itself with greater capability to respond to cyber threats, CAMP aims to provide more opportunities for information and knowledge learning, project assistance, and collaborative action in a global among members.

Appendix 4 | Abbreviations

APCERT	Asia-Pacific Computer Emergency Response Team
CAMP	Cyber security Alliance for Mutual Progress
CISO	Chief Information Security Officer
DDoS	Distributed Denial of Service
FIRST	Forum of Incident Response and Security Teams
FSC	Financial Services Commission
FSI	Financial Security Institute
ICT	Information and Communications Technologies
IDC	Internet Data Center
IOT	Internet of Things
ISAC	Information Sharing and Analysis Center
ISMS	Information Security Management System
ITRC	Information Technology Research Center
KFTC	Korea Financial Telecommunications & Clearings Institute
K-ICT	Korea Information and Communications Technologies
KISA	Korea Internet & Security Agency
KISC	Korea Internet Security Center of the KISA
KOSCOM	Korea Securities Computing Corporation
KrCERT/CC	Korea Computer Emergency Response Team Coordination Center
MND	Ministry of National Defense
MOE	Ministry of Education
MOGAHA	Ministry of Government Administration and Home Affairs
MOHW	Ministry of Health & Welfare
MOLIT	Ministry of Land, Infrastructure, and Transport
MOMAF	The Ministry of Maritime Affairs & Fisheries
MOTIE	Ministry of Trade Industry and Energy
MSIP	Ministry of Science, ICT and Future Planning
NCSC	National Cyber Security Center of the NIS
NIS	National Intelligence Service
NSO	National Security Office of the Blue House
NSR	National Security Technology Research Institute